CLAIMS:

1. A method for establishing a system for secure communications between nodes in a workgroup over a public network by facilitating the creation of a virtual private network (VPN), including a VPN server, the method comprising the steps of:

establishing a secure connection between at least a pair of nodes within said workgroup and said VPN server; and

synchronizing each of said connected nodes with said VPN server such that each of said connected nodes receives configurational information relating to attributes of each of said other connected nodes;

wherein, when an attribute relating to one of said connected nodes or said VPN server is revised, said configurational information relating to said attribute is updated at each of said connected nodes.

2. The method for establishing the system of claim 1, further comprising, following said step of establishing said secure connection, a step of authorizing, at said VPN server, validity of said connection between said VPN server and each of said connected nodes.

3. The method for establishing the system of claim 1, wherein following said step of synchronizing said server and each of said connected nodes, a step of sensing attribute revisions relating to one of said connected nodes or said server.

4. The method for establishing the system of claim 1, wherein said VPN server enables secure exchange of said configurational information between said connected nodes.

5. The method for establishing the system of claim 1, wherein said VPN server restricts exchanges of configurational information based on trust relationships established by said connected nodes.

6. The method for establishing the system of claim 1, wherein each of said connected nodes remains in a loop with said VPN server so as to forward any attribute revisions changes within a node to each of said connected nodes.

7. The method for establishing the system of claim 1, wherein each of said connected nodes automatically pull changes from said VPN server so as to update said configurational information stored at said node.

8. A system for establishing secure communication between nodes in a workgroup over a public network by facilitating the creation of a virtual private network, the system comprising:

at least a pair of nodes;

a VPN server, connected with each of said at least a pair of nodes for synchronizing each of said connected nodes with said VPN server such that each of

said connected nodes receives configurational information relating to attributes of said other connected nodes or said VPN server;

wherein, when an attribute relating to one of said connected nodes or said server is revised, said configurational information relating to said attribute is updated at each of said connected nodes.

9. The system of claim 8, wherein said system further comprises a datastore connected to said server.

10. The system of claim 8, wherein said system further comprises a client application located at each of said connected nodes.

11. A method for establishing a system for secure transfer of a data packet between a first node and a second node in a workgroup over a public network, where said nodes are members of a virtual private network, the method comprising the steps of:

assessing a presence of a device associated with said connected first and second nodes;

modifying a packet header of said data packet intended for transfer between said first and second nodes when a device is detected;

wherein said modification of said packet headers facilitates traversing said detected device for transmission of said data packet between said first node and said second node.

12. The method for establishing the system of claim 11, wherein said modified packet header comprises an Encapsulated Security Payload (ESP) header, an Internet Protocol (IP) header, and a masquerade bit, said masquerade bit acting as an indicator to one of said first and second nodes that said data packet has been modified.

13. The method for establishing the system of claim 12, wherein said masquerade bit is located between said ESP header and said IP header.

14. The method for establishing the system of claim 12, wherein a packet interception mechanism analyses said packet headers for detecting the presence of said masquerade bit.

15. The method for establishing the system of claim 13, wherein when said masquerade bit is detected within said packet header, said modified packet header is removed and the original packet header of said data packet routes said data packet to one of said first and second node.

16. The method for establishing the system of claim 11, wherein said device is selected from a group comprising a Network Address Translation (NAT) Device, a firewall, a gateway, a proxy server, and combinations thereof.

17. The method for establishing the system of claim 11, wherein when a device is detected, said device is located in front of said node.

18. A computer system for establishing the secure transfer of a data packet between nodes in a workgroup over a public network, where said nodes are members of a VPN, the system comprising:

a first node;

a second node;

a device detection mechanism; and

a packet interception mechanism;

wherein when a data packet is transferred from said first node to said second node and a device is detected at said second node, said data packet is intercepted and a packet header of said data packet is modified to facilitate the data transfer between said nodes.